DRAFT

Statement of Work
to
Contract PCH*XXXXX*
for
Information Technology Security Review
&
Compliance Audit

The successful proposer will demonstrate an understanding of the objectives for the IT Security Review and Compliance Audit and will provide AOC with an approach that demonstrates understanding of industry best practices and experience in similar projects. Vendor must propose to provide AOC with services and deliverables in the following categories:

- *Project Management.*
- *Evaluation of AOC IT Security Policies and Practices.*
- *Penetration Testing – Internal and External.*
- *Vulnerability Assessment and Risk Analysis.*
- *Control Design Review.*
- *Social Engineering Mechanism.*

These services and related tasks are described in more detail in the following sections. ATTACHMENT A must be used as a reference to properly prepare a response to the procurement. Following select of the Apparent Successful Vendor (ASV), the Statement of Work (SOW) will be mutually negotiated by ASV and AOC. A final version of the SOW will be incorporated in to the contract prior to execution by both parties.

This Statement of Work (SOW) is made and entered by and between the Administrative Office of the Courts ("AOC"), and *[Vendor]* ("Vendor"), for Information Technology (IT) Security Review and Compliance Audit.

This SOW incorporates by reference the terms and conditions of Contract Number PCH*[XXXXX]* in effect between the AOC and Vendor. In case of any conflict between this SOW and the Contract, the Contract shall prevail. AOC and Vendor agree as follows:

1. Introduction

The primary deliverables under this SOW are related to Information Technology Review and Compliance Audit. The services provided under this SOW are required as AOC continuously must meet the demands of court customer changes and modifications, which may introduce vulnerabilities that were previously non-existent. Consequently, periodic audit of information systems must be carried out by an independent, competent party. Keeping AOC's existing systems running as securely as possible is a top priority for AOC and the courts. See RFP Section Information regarding AOC's

IT Portfolio Summary, which provides an overview of our technology infrastructure. A schematic depiction of the network is included in **Attachment B**.

2. Project or Task Objectives

Vendor must provide services and deliverables, and otherwise do all thing necessary for or incidental to the performance of work as set forth under this SOW for all services as provided below:

- Project Management.
- Evaluation of AOC IT Security Policies and Practices.
- Penetration Testing – Internal and External.
- Vulnerability Assessment and Risk Analysis.
- Control Design Review.
- Social Engineering Mechanism.
- Security Plan.

3. Scope of Work and Deliverables

Vendor shall provide Services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below.

Vendor shall produce the Deliverables as provided in the Tasks as described below.

Task 1: Vendor Project Management

The scope of Task 1 shall include the following required activities:

1) Be the primary point of contact to AOC on all IT Security-related guidance, issues, and concerns.
2) Conduct an initial planning meeting with AOC prior to the start of the project.
3) Complete change-request documentation as required.
4) Manage AOC expectations and satisfaction throughout the project.
5) Schedule and coordinate the necessary resources to support the project.
6) Identify, escalate and document project issues as necessary.
7) Provide Vendor team guidance and planning.
8) Create and maintain a project plan in conjunction with AOC and measure weekly progress against mutually agreed-upon milestones.
9) Participate, along with Vendor team staff, in regularly scheduled Team update/status meetings (as determined needed by the Team).
10) Prepare written status reports for AOC at mutually agreed-upon intervals.
11) Attend weekly team status meeting onsite at AOC; delegation to other Vendor staff only with prior approval by AOC Project Manager.

Deliverables -Task 1

Deliverables related to Task 1 shall be completed no later than *[Month Date], 2013.*

1) Provide bi-weekly project status report to AOC PM for review and consideration.
2) Participate in project team status meetings.
3) Present Final Assessment and Analysis Report to ISD Management and other stakeholders, as required.

Task 2: Evaluation of AOC IT security policies and practices

The scope of Task 2 shall require Vendor to provide evaluation of AOC IT security policies against industry best practices and standards.

1) All tasks shall be completed by Vendor CISSP-certified staff resource(s).
2) Identification gaps and report findings to AOC PM with recommendations for remediation.

Deliverables - Task 2

Deliverables related to Task 2 shall be completed no later than *[Month Date]*, 2013.

1) Submit draft Policy Review and Evaluation Report identifying gaps and providing recommendations for remediation to AOC Project Manager for review and consideration.
2) Submit final Policy Review and Evaluation Report identifying gaps and providing recommendations for remediation to AOC Project Manager for review and final acceptance.

Task 3: Penetration Testing

A vital component in the assessment of the efficiency of perimeter defenses for a network environment is an external vulnerability and network penetration test. In order to conduct daily work functions, any business must maintain a connection to the Internet which requires protections such as firewalls and other security precautions. Additional, as the primary provider of systems to our court stakeholders it is critical to look at all information available about AOC from the Internet to ensure private data remains confidential.

Task 3a: External /Internet Penetration Testing Assessment

Vendor shall complete the External/Internet Penetration Testing with very little information provided by AOC itself. Vendor shall complete assessment by imitating a "hacker" with no inside information regarding AOC systems present or technologies currently in use.

Vendor shall complete the External/Internet Penetration Testing Assessment using the following test types:

1) Search for publicly available information using Internet, newsgroup postings, etc.
2) Search domain registration for useful information.
3) Retrieve public Domain Name Service (DNS) records.
4) Identify systems accessible over the Internet (i.e., web, email, etc.).
5) Conduct port scans.

6) Identify running services.
7) Conduct Simple Network Management Protocol (SNMP) scans.
8) Identify operating systems if possible.
9) Identify web and email service versions.
10) Enumerate systems if possible.
11) Attempt to utilize remote access protocols if available.
12) Email server analysis (i.e., open relay, anonymous email, etc.).
13) Web server analysis (i.e., default configuration, sample scripts, etc.).
14) Website and web application analysis.
15) Conduct vulnerability scans of systems and network devices.
16) Exploit systems when possible.
17) Evaluate test results and identify false positives.

Task 3b: Internal/Physical Penetration Assessment

Vendor shall complete the Internal/Physical Penetration Testing by simulating an attack originating from with AOC's network perimeter defenses with very little information provided by AOC itself. Vendor shall complete assessment by imitating a "hacker" with no inside information regarding AOC systems present or technologies in use.

Vendor shall complete the Internal/Physical Penetration Testing Assessment using the following test types:

1) Internal DNS configuration.
2) Identify subnets and network architecture.
3) Systems enumeration.
4) Default or weak authentication configurations.
5) Port scans.
6) Identify running services.
7) Validate authentication requirements for non-public information.
8) Test system patch levels for currency.
9) Identify weak protocols used in the environment.
10) Conduct vulnerability scans of systems and network devices.
11) Exploit systems when possible.
12) Evaluate test results and identify false positives.

Deliverables - Task 3

Deliverables related to Task 3 shall be completed no later than *[Month Date]*, 2013.

1) Submit *draft* External Penetration Testing Assessment Report including threat resistance validation to AOC Project Manager for review and consideration.
2) Submit *draft* Internal Penetration Testing Assessment Report to AOC Project Manager for review and consideration.
3) Submit *final* External Penetration Testing Assessment Report including threat resistance validation to AOC Project Manager for review and final acceptance.
4) Submit *final* Internal Penetration Testing Assessment Report to AOC Project Manager for review and final acceptance.

Task 4: Vulnerability Assessment and Risk Analysis

The required activities to complete the Vulnerability Assessment and Risk Analysis shall require full collaboration between Vendor and AOC PM as well as other organizational personnel to ensure comprehensive testing of all aspects of information security has been analyzed.

1) Perform risk assessment, which will document reasonable and foreseeable threats to the AOC and well as controls in place to migrate those threats.
2) Controls will be tested through sampling to determine effectiveness.
3) Vulnerability assessment and risk analysis shall include, but not limited to, the following test types:
    a. Validate physical security controls around sensitive systems.
    b. Verify environmental protection against, fire, flood and other hazards.
    c. Verify antivirus software deployment and maintenance.
    d. Review user account administration procedures and practices.
    e. Review firewall filtering rule configurations.
    f. Validate separation of suited and dual control issues.
    g. Assess encryption methodologies used.
    h. Validate controls over software licensing.
    i. Evaluate data destruction procedures.

Deliverables - Task 4

Deliverables related to Task 4 shall be completed no later than *[Month Date]*, 2013.

1) Submit draft Risk Assessment and Control Design Review Report to AOC Project Manager for review and consideration.
2) Submit draft Control Testing and Gap Analysis to AOC Project Manager for review and consideration.

3) Submit final Risk Assessment and Control Design Review Report to AOC Project Manager for review and final acceptance.

4) Submit final Control Testing and Gap Analysis to AOC Project Manager for review and final acceptance.

Task 5: Control Design Review

Under this task, Vendor shall review application controls to determine whether current security policies and procedures provide the following:

1) Assurance that data is input and processed accurately and completely,

2) Limit personnel to only the electronic access necessary to perform their assigned duties,

3) Reduce the risk of damage, loss, unauthorized use and modification of resources, and

4) Proper recognition, handling and education around managing sensitive data.

As part of this deep IT security analysis, Vendor will be required to perform three (3) separate analyses of different business units within AOC's Information Services Division. Each business unit holds different roles and responsibilities for maintaining security for the agency's network and applications.

Task 5a: Data Warehouse Risk Analysis

Vendor shall complete an analysis of the Data Warehouse and associated applications. This includes, but is not limited to, ETL tool, end user query tool, and data extraction and dissemination.

Vendor shall complete Contract Design Review for AOC Data Warehouse through analysis of the following:

1) The Extract Transform and Load (ETL) process ensuring data is processed accurately and completely.

2) The access control and admin process ensuring that access is appropriately restricted and managed.

3) The overall design and implementation of the Date Warehouse applications to determine whether unaddressed significant risk exists to the Data Warehouse and supporting tools from the confidentiality, integrity and availability perspectives.

Task 5b: Infrastructure Risk Analysis

Vendor shall complete an analysis of Infrastructure and associated applications. This includes, but is not limited to, databases, network design and segmentation, intrusion prevention and detection, file servers, and mail servers.

Vendor shall complete Contract Design Review for Infrastructure through analysis of the following:

1) The access control and admin process ensuring that access is appropriately restricted and managed.

2) The overall design and implementation of the Infrastructure applications to determine whether unaddressed significant risk exists to AOC Infrastructure and supporting tools from the confidentiality, integrity and availability perspectives.

Task 5c: Operations Risk Analysis

Vendor shall complete an analysis of Operations and associated applications. This includes, but is not limited to, web applications, mainframe applications, data and file sharing.

Vendor shall complete Contract Design Review for Operations through analysis of the following:

3) The access control and admin process ensuring that access is appropriately restricted and managed.
4) The overall design and implementation of the Operations applications to determine whether unaddressed significant risk exists to the data warehouse and supporting tools from confidentiality, integrity and availability perspectives.

Deliverables – Task 5

1) Submit *draft* Data Warehouse Risk Audit Report to AOC Project Manager for review and consideration.
2) Submit *draft* Infrastructure Risk Audit Report to AOC Project Manager for review and consideration.
3) Submit *draft* Operations Risk Audit Report to AOC Project Manager for review and consideration.
4) Submit *final* Data Warehouse Risk Audit Report to AOC Project Manager for review and final acceptance.
5) Submit *final* Infrastructure Risk Audit Report to AOC Project Manager for review and final acceptance.
6) Submit *final* Operations Risk Audit Report to AOC Project Manager for review and final acceptance.

Task 6: Social Engineering Mechanisms

Vendor shall conduct an assessment of the security awareness of employees to determine additional network vulnerabilities and potential risks. Vendor through random sampling will conduct this assessment using the following tests:

1) Vendor staff will pose as AOC IT staff or other authorized individuals and attempt to gain access to sensitive areas of the organization's infrastructure.
2) Vendor staff will perform an email-based attack attempting to entice AOC employees into opening or downloading an attachment from an external email address or providing sensitive data such as their authentication credentials.
3) Vendor staff will perform a telephone-based testing of AOC employee awareness by requesting passwords or other sensitive information of employees over the phone.

Deliverables - Task 6

Deliverables related to Task 6 shall be completed no later than *[Month Date]*, 2013.

1) Submit *draft* Social Engineering Mechanism Report which includes findings and recommendations for remedy to AOC Project Manager for review and consideration.
2) Submit *final* Social Engineering Mechanism Report to AOC Project Manager for review and final acceptance.

Task 7: Security Plan

Vendor shall conduct a thorough IT security analysis and audit of AOC. Vendor must describe the methodology and associated tools and strategies it will use to develop a detailed IT security plan for AOC.

Deliverables - Task 7

Deliverables related to Task 7 shall be completed no later than *[Month Date]*, 2014.

1) Submit *draft* Security Plan which includes findings and recommendations for remedy to AOC Project Manager for review and consideration.
2) Submit *final* Security Plan to AOC Project Manager for review and final acceptance.

4. Timeline and Period of Performance

The period of performance for this project will start on within five (5) business days of contract execution with AOC with the SOW tasks to be completed no later than *[Month Date]*, 2014. AOC has the right to extend or terminate this SOW at its sole discretion.

5. Task Deliverables Schedule

Acceptance criteria is set forth in Section 14 of Contract PCH*XXXXX* . At a minimum, Vendor shall provide each draft deliverable to AOC Project Manager for review and consideration no later than the due date set forth in the Task Deliverables Schedule below. If requires additional modifications to a draft deliverable, AOC Project Manager will notify Vendor Project Manager of all required edits before AOC Project Manager will provided acceptance of any such deliverable as final. Documents provided to AOC Project Manager as FINAL deliverables shall be marked as such and shall be due no later than the due date set forth in the Task Deliverables Schedule below.

The table below will be completed based on the dates provided by Vendor in the Project Plan and schedule submitted as part of any proposal. If selected as ASV, Vendor should expect potential contract negotiations with AOC regarding adjustment to proposed deliverable due dates.

Task No.	Task Deliverables	Deliverable Due Date
1	Project Management Bi-weekly Status Report	Bi-weekly, 5 PM PST Monday
1	Attend IT Security Project Team Meeting	Weekly, as required
2	Draft Policy Review and Evaluation Report	*MM/DD/YYYY*
2	Final Policy Review and Evaluation Report	*MM/DD/YYYY*
3a	Draft External Penetration Testing Assessment	*MM/DD/YYYY*

	Report	
3b	Draft Internal Penetration Testing Assessment Report	*MM/DD/YYYY*
3a	Final External Penetration Testing Assessment Report	*MM/DD/YYYY*
3b	Final Internal Penetration Testing Assessment Report	*MM/DD/YYYY*
4	Draft Risk Assessment and Control Design Review Report	*MM/DD/YYYY*
4	Draft Control Testing and Gap Analysis	*MM/DD/YYYY*
4	Final Risk Assessment and Control Design Review Report	*MM/DD/YYYY*
4	Final Control Testing and Gap Analysis	*MM/DD/YYYY*
5a	Draft Data Warehouse Risk Analysis Report	*MM/DD/YYYY*
5b	Draft Infrastructure Risk Analysis Report	*MM/DD/YYYY*
5c	Draft Operations Risk Analysis Report	*MM/DD/YYYY*
5a	Final Data Warehouse Risk Analysis Report	*MM/DD/YYYY*
5b	Final Infrastructure Risk Analysis Report	*MM/DD/YYYY*
5c	Final Operations Risk Analysis Report	*MM/DD/YYYY*
6	Draft Social Engineering Mechanism Report	*MM/DD/YYYY*
6	Final Social Engineering Mechanism Report	*MM/DD/YYYY*
7	Draft Security Plan	*MM/DD/YYYY*
7	Final Security Plan	*MM/DD/YYYY*

Changes to this SOW shall be mutually agreed upon in writing and incorporated into the contract through execution of an amendment signed by both parties.

6. Compensation and Payment

AOC shall pay Vendor an amount not to exceed *[_____]* dollars *($___) [specify maximum dollar amount]* for the performance of all activities necessary for or incidental to the performance of work as set forth in this SOW. Vendor's compensation for services rendered shall be based on Vendor's Prices as set forth in *Table 2 – Payment Schedule* below.

Task No.	Key Deliverables*	Payment
2	FINAL Policies Review and Evaluation Report	*$ xx,xxx*
3a	FINAL External Penetration Testing Assessment Report	*xx,xxx*
3b	FINAL Internal Penetration Testing Assessment Report	*xx,xxx*
4	FINAL Risk Assessment and Control Design Review Report	*xx,xxx*
4	FINAL Control Testing and Gap Analysis	*xx,xxx*
5a	FINAL Data Warehouse Risk Analysis	*xx,xxx*

5b	FINAL Infrastructure Risk Analysis	*xx,xxx*
5c	FINAL Operations Risk Analysis	*xx,xxx*
6	FINAL Social Engineering Mechanism Report	*xx,xxx*
7	FINAL Security Plan	*xx,xxx*
	Contract Total	***$ xx,xxx***

*Costs associated with services related to Vendor Project Management shall be considered inclusive of these deliverables.

Table 2 – Payment Schedule

AOC shall not reimburse Vendor for any travel and other expenses incurred in performing work under this SOW.

7. Vendor Staff, Roles and Responsibilities

[Identify Vendor staff who will be involved, naming individuals key to the project, and describe in detail their roles and responsibilities.]

Vendor's Personnel

For work to be performed for AOC, AOC reserves the right to reject any of the Vendor employees. Any and all costs or expenses associated with replacement of any person or entity shall be borne by the Vendor.

Vendor may not change or replace any of the staff assigned to this Contract without prior approval of AOC, which approval will not be unreasonably withheld. Vendor is not responsible for delays or repeated tasks caused by factors outside its control. These factors include, but are not limited to, availability of AOC personnel, equipment, and telecommunication provider services.

Vendor will use commercially reasonable efforts to take into account AOC's schedule, but in all events the performance of Services is subject to the availability of Vendor personnel and resources, as determined by Vendor.

Vendor shall be responsible to ensure that all its employees are properly trained, certified, or licensed as appropriate and are properly qualified by education and experience to perform the work. Vendor shall avoid overstaffing the work or shuffling personnel assigned to said work.

During all work effort required to be performed under this SOW, Vendor is responsible to monitor all required certifications for assigned employees, maintain to proof of certification renewals during the term of the SOW.

Vendor will conduct work in the most appropriate location based on access requirements and costs associated with travel. Therefore, the external assessment and web application assessment will be conducted remotely to AOC's offices.

Vendor will perform discovery of AOC's Internet-accessible networks and systems, but will confirm this information with the customer before proceeding. Notification will be provided by the Vendor through email with a follow-up voice call to both the primary and secondary AOC SME contacts.

Vendor will participate in presentations for AOC executive management and the steering committees, as required.

Vendor will provide the applicable and necessary labor, consultation, materials, project management and/or tools to perform the Services and provide the Deliverables described herein.

Vendor Project Manager

Vendor Project Manager shall be responsible for defining the project scope and estimate, building the detailed project plan, monitoring and directing project activities as they relate to the project scope and project plan. He shall be required to document scope changes through the change management process, and coordinating the daily tasks of the project team. Vendor Project Manager contact information is provided below.

Vendor Project Manager: *<Last Name, First Name>*
Address: *Street Address, City, State, Zip Code+4*
Phone: (XXX) XXX-XXXX Fax: (XXX) XXX-XXXX Email: *<email address>*

Vendor Account Manager

Vendor Account Manager will be the principal point of contact for AOC concerning Vendor's performance under this Contract. Vendor shall notify the Project Manager, in writing, when there is a new Vendor Account Manager assigned to this Contract. The Vendor Account Manager contact information is:

Vendor Account Manager: *<Last Name, First Name>*
Address: *Street Address, City, State, Zip Code+4*
Phone: *(XXX) XXX-XXXX* Fax: (XXX) XXX-XXXX E-mail: *<email address>*

***Additional Requirements** (Optional)*

<This optional section can be completed following contract negotiations with ASV. >

8. AOC Staff, Roles and Responsibilities

AOC Project Manager, *<Name>,* for this project shall be responsible for coordinating resources and staff in support of project activities, and will provide technical assistance and guidance for the business and technology areas of the project. AOC Project Manager will make final project decisions and have acceptance signoff authority for all project deliverables.

9. Additional Terms and Conditions Specific to this SOW

Vendor will work collaboratively with all necessary project leadership, project staff and project partners assigned to this project. Work products produced by the Vendor for AOC will become the property of AOC. Vendor must be able to work collaboratively with AOC and project partners to gain understanding of their business needs.